DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

Docket No. TSA-2004-19166
Privacy Act Notice
Transportation Security Threat Assessment System and
Transportation Worker Identification Credentialing System

COMMENTS OF THE ELECTRONIC PRIVACY INFROMATION CENTER

By notice published on September 24, 2004, the Department of Homeland Security ("DHS") announced that the Transportation Security Administration ("TSA") is altering two existing systems of records.[1] According to the notice, the Transportation Security Threat Assessment System ("T-STAS"—DHS/TSA 002) "facilitates the performance of threat assessments and employment investigations on individuals who require special access to the transportation system," and the Transportation Worker Identification Credentialing System ("TWIC"—DHS/TSA 012) "facilitates the testing and evaluation of certain technologies and business processes associated with access control for transportation workers requiring unescorted access to secure areas of transportation facilities."[2] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") files these comments to illustrate that, while the stated purposes of these two programs are narrowly drawn to transportation security, some provisions require close attention to ensure that these systems do not fall into the traps of unintended uses and mission creep.

Introduction

[1] Privacy Act Notice, 69 Fed. Reg. 57348 (Sept. 24, 2004).

[2] *Id*. at 57349.

Currently in its prototype phase, TWIC is an identification card that is issued to transportation workers, authorized visitors, and all other persons requiring unescorted access to transportation infrastructure secure areas.[3] Those seeking access to certain areas of airports, rail facilities, port facilities, port headquarters, and pipelines will require the TWIC card to enter.[4] A central TWIC database maintained by TSA stores personal information and validates a person's eligibility to enter these areas.[5] The central TWIC database will also be used to conduct background checks and compare a person's identity against other national "watch list" threat-intelligence databases.[6] Persons required to have TWIC identification cards will include foreign merchant mariners and foreign truck drivers.[7] TWIC stores data on an identification card carried by each transportation employee.[8] These cards are required for entry through Access Control Points, which grant access to certain areas by matching the data stored on the card with data stored at the central TSA data center.[9] Access Control Points include vehicle gates, truck lanes, personnel turnstiles, building doors, and pedestrian entrances.[10]

---

[3] 68 Fed. Reg. 49508 (August 18, 2003).

[4] Transportation Security Administration, *Transportation Worker Identification Credential (TWIC) Stakeholder Brief* (July 2003) available *at* <http://www.uscg.mil/hq/g-m/advisory/merpac/TSA-TWIC-Stakeholder-Brief.pdf> (hereinafter "TWIC Stakeholder Brief").

[5] TWIC Stakeholder Brief, *supra*.

[6] *Security Credentials for Port Personnel Before the House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation*, 107th Cong. (Feb. 13, 2002) (statement of Rear Admiral James Underwood); TWIC Stakeholder Brief, *supra* at 10-11.

[7] *Id*.

[8] *Id*.

[9] *Id.*

[10] *Id*.

The pilot project implementation of the TWIC database contains a substantial amount of sensitive personal information. Specifically, the TWIC database includes the following data elements:

Name
Address
Phone Number
Social Security Number
Date of Birth
Place of Birth
Administrative Identification Code
Unique Card Serial Number
Systems Identification Code
Company/Organization Affiliation
Issue Date
Biometric data
Photographic data
Access Level Information
Expiration Date[11]

This data is stored at Regional Database and Issuance centers and a centralized TSA data center.[12] The central TSA data center matches individuals against persons appearing in national "watch list" database, and revokes access to all TWIC facilities from such persons.[13]

T-STAS was originally known as the Transportation Workers Employment Investigations System.[14] This program will collect much of the same information as TWIC, as well as physical descriptions, date, place and type of flight training, travel document information, crew status, and compilations of criminal history obtained from

[11] Privacy Act Notice, *supra* at 57351.

[12] TWIC Stakeholder Brief, *supra* at 10-11.

[13] *Id.* at 12.

[14] Privacy Act Notice, *supra* at 57349.

the FBI's Fingerprint Identification Records System.[15] This data will be used to perform security threat assessments and employment investigations, and to permit those results to be retrieved "in other governmental, commercial, and private data system".[16]

A. The Sensitivity of the Stored Information Requires Stringent Safeguards

Both T-STAS and TWIC gather highly sensitive personal information about a large number of people directly or tangentially related to the U.S. transportation industry. EPIC understands that the collection of this information may be necessary to ensure that those with ill intent do not gain access to our transportation infrastructure. However, TSA must take into consideration the privacy interests of those whose information is gathered by T-STAS and TWIC, and take great care to guard this information from excessive use, misuse, or even use in furtherance of a terrorist act.

The information TSA gathers for T-STAS and TWIC has the potential to pose a serious threat to personal privacy and the stated goals of the programs if it is used in ways unrelated to transportation security. The inclusion of the Social Security Number is especially problematic because it was never intended to be used as an identifier, and its disclosure gives rise to the risk of identity theft.[17] The use of biometric identifiers carries its own risk of misidentification and privacy invasion.[18] TSA must strictly adhere to its stated commitment to safeguard this information from misappropriation and improper use.

---

[15] *Id*. at 573490-57350.

[16] *Id*. at 57350.

[17] For more information on the importance of Social Security number confidentiality, *see* EPIC's Social Security Number page, *available at* http://www.epic.org/privacy/ssn.

[18] For more information on the problems associated with biometric identifiers, *see* EPIC's Biometrics page, *available at* http://www.epic.org/privacy/biometrics.

Of particular concern is T-STAS' routine use (4), which allows the information to be accessed by "contractors, grantees, experts, consultants, volunteers, or other like persons when necessary to perform a function or service related to this system of records."[19] In the event that the dissemination of this data to a TSA contractor is necessary, the Privacy Act expressly provides that the contractor must observe Privacy Act obligations just as the TSA would.[20] More distressing is the notion that such sensitive information will be available to "grantees, experts, consultants, volunteers, or other like persons[.]" Despite the notice's assurance that "[s]uch recipients are required to comply with the Privacy Act," it is not at all apparent that they are legally bound to observe the Privacy Act obligations that apply to the government and government contractors. Those who do not have the minimum personal investment of employment or contract status with TSA should not have access to sensitive personal data.

B. <u>TSA Must Adhere to the Principles of the Privacy Act</u>

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[21] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[22]

---

[19] Privacy Act Notice, *supra*. at 57350.

[20] 5 U.S.C. 552a(m) (2004).

[21] Pub. L. No. 93-579 (1974).

[22] *Id*.

Last year, DHS's Chief Privacy Officer touted the protections afforded by the Privacy Act, explaining that the law:

> provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, though detailed 'system of records' notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.[23]

EPIC applauds the fact that TSA does not claim any Privacy Act exemptions for TWIC, thus affording the individuals affected by the system the full protection of the law. However, TSA has claimed unexplained exemptions for T-STAS, and this requires clarification. The notice merely states that "[p]ortions of this system are exempt under 5 U.S.C. 55a(k)(1) and (k)(2)."[24] Nowhere does the notice state what portions are exempt or under what rationale. These issues must be addressed in order for individuals to know what rights they have in their personal information collected and maintained in the system, and what obligations the agency must observe under law.

C. Routine Uses Must Be More Narrowly Drawn to Prevent Mission Creep and Abuse

The Privacy Act Privacy Act requires that TSA "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[25] In adopting the Privacy Act, Congress was clear

[23] Remarks of Nuala O'Connor Kelly Before the 25th International Conference of Data Protection and Privacy Commissioners, Sydney Australia, September 11, 2003.

[24] Privacy Act Notice, *supra*. at 57350.

[25] 5 U.S.C. § 552a(e)(1) (2004).

in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision:

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][26]

As the Office of Management and Budget noted in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[27]

The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government's stated and legally authorized objective. This notice does not assert that either T-STAS or TWIC is exempt from this requirement.[28] TSA must take great care to ensure that both collections do not become error-filled, invasive repositories of all sorts of information bearing no relationship to their stated goal of facilitating "the performance of security threat assessments and other investigations that TSA may conduct to ensure

---

[26] S. Rep. No. 93-3418, at 47 (1974).

[27] Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28960 (July 9, 1975).

[28] Although, as explained *supra*, TSA has claimed unidentified exemptions under the Privacy Act with no further explanation. It is possible, therefore, that 5 U.S.C. § 552a(e)(1) is one of the exemptions TSA has claimed for T-STAS.

transportation security."[29] It was exactly this "mission creep" that caused the failure of the second-generation Computer Assisted Passenger Prescreening System (CAPPS II).[30]

TWIC's routine use (1) allows dissemination of information:

> To the appropriate Federal, State, local, tribal territorial, foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.[31]

This, language, which is repeated in routine use (2) of T-STAS, far exceeds what is "relevant and necessary" to achieve the program's purpose. While this use could be employed to address a legal violation related to transportation security, it is not narrowly drawn to serve only that purpose. In fact, under this language, *any* violation or even *potential* violation of the law may justify the dissemination of sensitive personal information to law enforcement agencies. The violation may be civil or criminal. It may have no relation at all to the transportation industry. Indeed, it may not even be a violation at all, but merely an undefined and highly subjective "potential" violation. This clearly goes beyond that which is "relevant and necessary" to maintain transportation security.

Routine use (5) of T-STAS also carries the potential to exceed what is "relevant and necessary" to achieve the program's stated purpose. This use grants access to personal information:

> To a Federal, State, local, tribal, territorial, foreign, or international agency, where such agency has requested information relevant or

[29] Privacy Act Notice, *supra* at 57350.

[30] Matthew L. Wald and John Schwartz, *Screening Plans Went Beyond Terrorism*, N.Y. Times, Sept. 19, 2004, at A35.

[31] Privacy Act Notice, *supra* at 57351.

> necessary for the hiring or retention of an individual, or the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefit.[32]

This broad language, which is loosely reflected in routine use (2) of TWIC,[33] would permit virtually any government entity access to personal information for a wide variety of reasons. The purpose of this system is to safeguard transportation security. Permitting a routine use that can be interpreted to allow government agencies at any level to access this information reaches far beyond that goal and into the realm of mission creep. Further, the phrase "or other benefit" can be expansively interpreted to allow access for purposes entirely unrelated to the hiring process. This language, which does not appear in the routine uses of TWIC, must be narrowed severely or discarded altogether from the routine uses of T-STAS.

D. Risk of Misuse of Data for Purpose that Could Endanger Travel Safety

Finally, we note that the widespread availability of the detailed information that will be used to determine access to sensitive travel areas poses the direct risk that this information, in the wrong hands, could enable precisely the threat to travel safety that these programs aim to prevent. In this era of widespread identity theft, we urge the agency to consider carefully the potential danger of disseminating the personal information of these individuals who are granted unescorted access to secure areas of transportation facilities.

Conclusion

EPIC stresses the importance of TSA's stated commitment to safeguarding the personal information collected under T-STAS and TWIC. However, for the foregoing

[32] *Id*. at 57350.

[33] *Id*. at 57351

reasons, the routine uses must be further narrowed to protect those who provide their sensitive personal information to these programs from the dangers of misappropriation and mission creep.

Respectfully submitted,

Marc Rotenberg
Executive Director

David L. Sobel
General Counsel

Marcia Hofmann
Staff Counsel

Paul Jones
IPIOP Law Clerk

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140